State of California
DEPARTMENT OF TRANSPORTATION

Business, Transportation and Housing Agency

Memorandum

Flex your power!
Be energy efficient!

To: ROBERT TRAVERSI
Chief Information Security Officer (Acting)
Division of Information Security and Operational Recovery

Date: December 8, 2009

File: P3010-615

ANN BARSOTTI
Deputy Director
Information Technology

ORIGINAL SIGNED BY:

From: GERALD A. LONG
Deputy Director
Audits and Investigations

Subject: FISMA Follow-up Review – Part II, Information Technology, Division of Information Security and Operational Recovery

SUMMARY

The California Department of Transportation's (Department) Audits and Investigations has completed a follow-up review of the issues identified in the report, "Audits of Internal Controls Pursuant to the Financial Integrity and State Manager's Accountability Act of 1983 (FISMA) for the 2006/2007 Cycle." This is a follow-up review and covers findings related to Information Technology (IT), the Division of Information Security and Operational Recovery (ISOR) covered under the IT Security and Risk Management (P3020-067) section of the FISMA report. The purpose of this review was to determine whether corrective actions have been taken and the reported findings were sufficiently addressed.

The review covered the period of July 1, 2007, to July 29, 2009. Our review was performed to verify that corrective actions to report findings had been completed as stated in the 60-, 180-, and 360-day status reports. Our verification procedures included interviews, observations, confirmations, review, and analysis of established processes, procedures, documents, and testing of supporting documentation provided.

REVIEW RESULTS

Our review disclosed that most of the corrective actions have been completed. However, we identified the following areas where the reported findings were not sufficiently addressed and/or where corrective actions were not fully completed:

1. State Administrative Manual (SAM) 5305.1 requires the Department to establish a risk analysis process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks. Given the complexity and ongoing nature of the risk management process, the Department has taken a phased-in approach. The Department has assigned the responsibilities for risk assessment to the Chief Information Security Officer, who contracted with an outside consultant to perform a risk assessment and produce a risk assessment report to identify risk areas and provide recommendations. The report was submitted to the Department's Director. In the next phase, the Department will need to identify the Department's information assets that are at risk, with particular emphasis on the applications of information technology that are critical to the Department's operations. In addition, the Department will need to estimate the cost of protective measures and select cost-effective security management measures to be implemented per SAM 5305, SAM 5305.1, and Deputy Directive (DD-80). Additionally, resources necessary for security management and the level of risk to be accepted by the Department need to be identified in the report submitted to the Department's Director.

2. ISOR provides the Information Security and Privacy Awareness Training for employees on its Web site annually. At the completion of the training, the employee receives a certificate of completion, which is automatically generated. In 2007, 45 percent of employees completed the Information Security and Privacy Awareness Training and in 2008, 57 percent of employees completed the training, indicating that ISOR has made continued progress. However, since 43 percent of employees in 2008 had not taken the training, it was determined that this finding has not yet been sufficiently addressed.

3. The prior audit identified that District 6 had operating water and sewage pipes above the computer equipment in the IT server room located in the basement. Since the issuance of the 2006/07 FISMA audit report, District 6 has taken some steps to address the audit finding. However, the relocation of the computer room has not yet taken place. The relocation is estimated to happen in early 2010. The relocation of the computer room needs to be completed to fully address the audit finding.

RECOMMENDATIONS

We request IT's ISOR prepare and provide a plan of action within 30 days to ensure that:

1. ISOR continue its effort and complete steps to ensure the Risk Management Program and risk assessment comply with SAM 5305, SAM 5305.1, and DD-80.

2. ISOR continue its efforts to coordinate training of all departmental employees and provide monitoring reports to Department management to full compliance.

3. District 6 complete its relocation of the computer room by June 30, 2010.

Pursuant to FISMA (Government Code sections 13400 through 13407), the above deficiencies will continue to be reported to the Department of Finance. Please provide our office with status reports on the implementation of audit finding dispositions 60, 180, and 360 days subsequent to the date of this letter. If all findings have not been corrected within 360 days, please continue to provide status reports every 180 days until the audit findings are fully resolved.

If you have any questions, please contact Zilan Chen, Audit Supervisor, at (916) 323-7877, or Laurine Bohamera, Chief, Internal Audits, at (916) 323-7107.

c: Randell H. Iwasaki, Director
Cindy McKim, Chief Deputy Director
Lori Guinan, Deputy Director Administration, District 6
Laurine Bohamera, Chief, Internal Audits, Audits and Investigations
Zilan Chen, Audit Supervisor, Audits and Investigations